Von der Theorie zur Praxis:

Die Auswahl eines Penetrationstests

Introduction // whoami

Fabian Mittermair

Head of Offensive Security

fabian.mittermair@certainity.com

Follow me on LinkedIn

Fabian Mittermair

Follow us on LinkedIn

CERTAINITY GmbH

CERTAINITY

CERTAINITY Mission

Als Cyber Security Spezialisten, unterstützen wir unsere Kunden dabei, ihre Informationssicherheit nachhaltig zu verbessern und ihr Kerngeschäft abzusichern.

CERTAINITY

Die Practices der CERTAINITY

OFFENSIVE SECURITY

DEFENSIVE SECURITY

PROCESS CONSULTING

SECURITY ENGINEERING

Kontaktieren Sie unmittelbar unsere Experten bei einem Cyber Security Vorfall

cert@certainity.com +43 664 888 44 686

CERTAINITY

Was ist der richtige Ansatz für mich?

Penetration Test

CERTAINITY

- Zielsetzung
- Scope
- Umfang
- Kenntnisstand
- Vorgehensweise & Tools

CERTAINITY

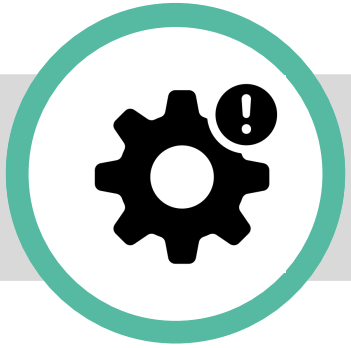
Typische Zielsetzungen (1/2)

Identifizierung von Schwachstellen

Aufdecken von möglichst vielen Schwachstellen, Sicherheitslücken oder unzureichend geschützte Bereiche in einem System oder Netzwerk.

Verbesserung des Sicherheitsniveaus

Basierend auf den Ergebnissen der Tests werden Schwachstellen behoben und Sicherheitsmaßnahmen verbessert



Überprüfung der Abwehrmechanismen

Prüfung der Wirksamkeit bzw. Effektivität der bestehenden Sicherheitsmaßnahmen.

Simulation

Simulation eines Angriffs um zu sehen, wie gut das Sicherheitsteam darauf reagiert und wie gut die Alarmierungs- und Reaktionsmechanismen funktionieren.

CERTAINITY

Typische Zielsetzungen (2/2)

Compliance

Einhaltung von geltenden Vorschriften und Compliance-Anforderungen

Schulung und Sensibilisierung

Schulungs- und Sensibilisierungs-Maßnahme, um das Bewusstsein für Sicherheitsrisiken zu schärfen und das Sicherheitsbewusstsein in der Organisation zu verbessern.

Validierung von Sicherheitsrichtlinien und -prozessen

Es wird überprüft, ob die Sicherheitsrichtlinien und -prozesse einer Organisation ordnungsgemäß implementiert und befolgt werden.

Vertrauen und Glaubwürdigkeit aufbauen

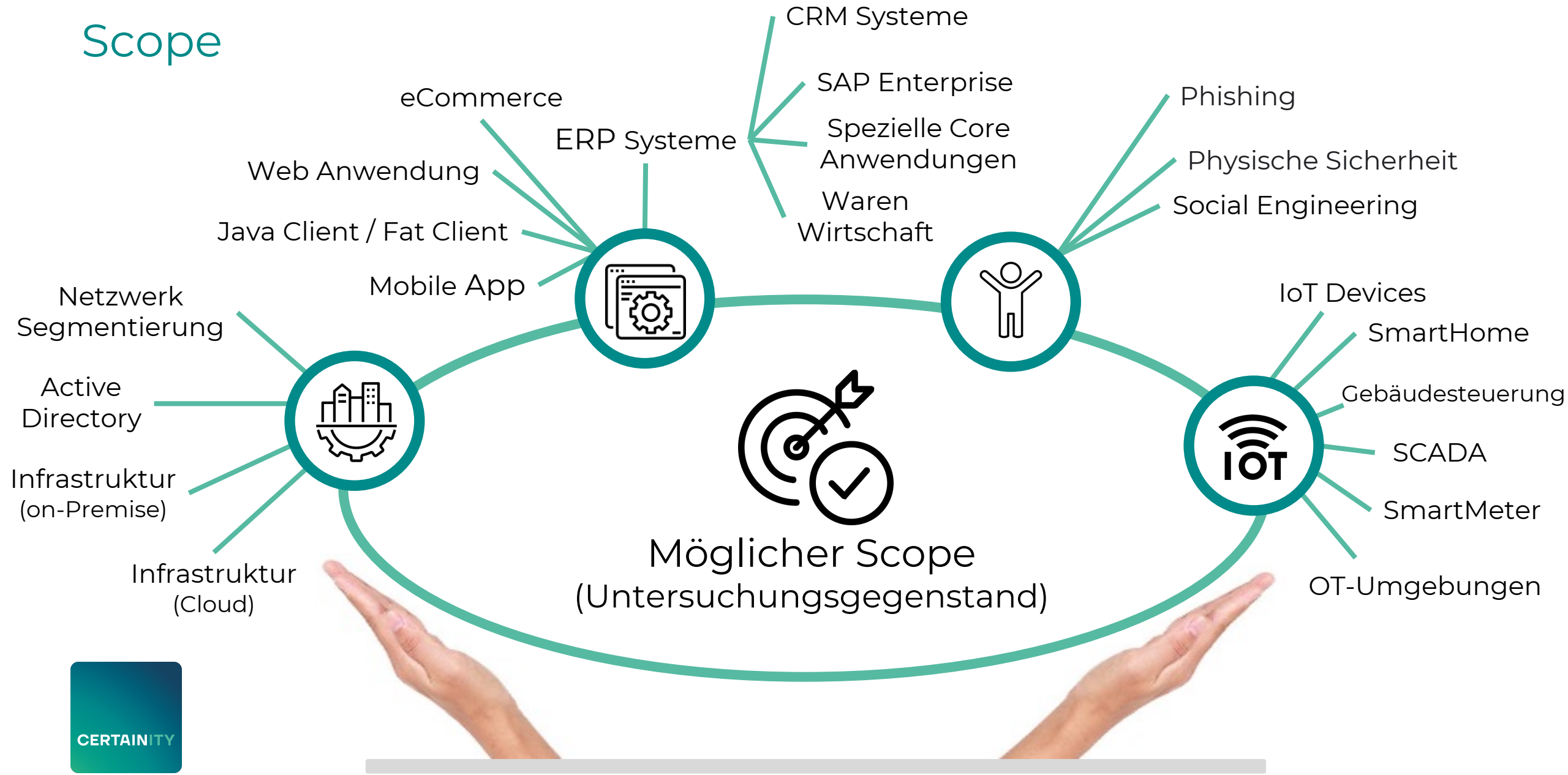
Durch regelmäßige Penetrationstests kann eine Organisation ihr Engagement für die Sicherheit ihrer Systeme und Daten demonstrieren und das Vertrauen von Kunden und Partnern gewinnen.

CERTAINITY

- Zielsetzung
- Scope
- Umfang
- Kenntnisstand
- Vorgehensweise & Tools

CERTAINITY

Scope

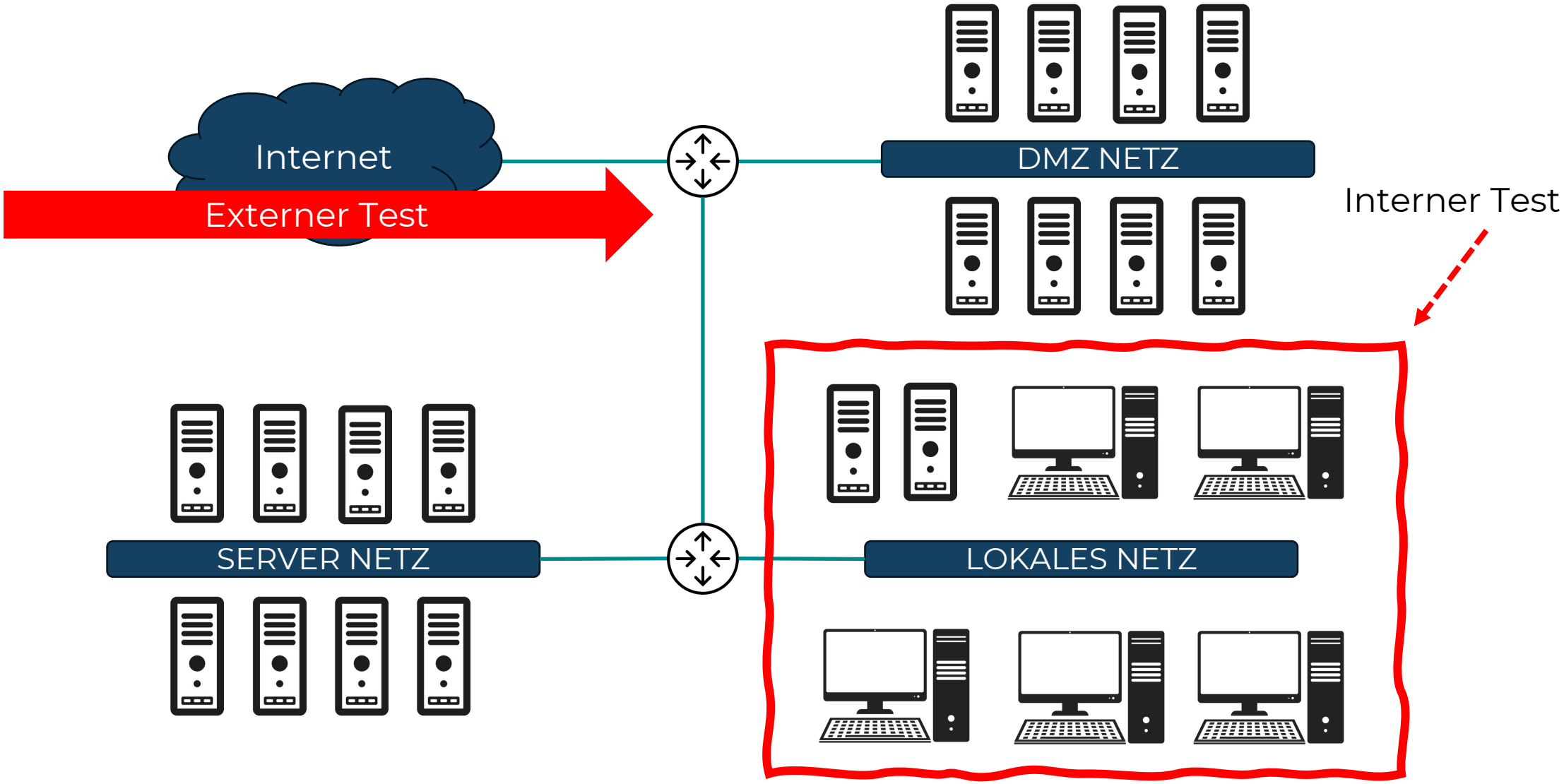


Extern / Außensicht
Ohne User-Accounts

Intern / Innensicht
Mit User-Accounts

CERTAINITY

Scope

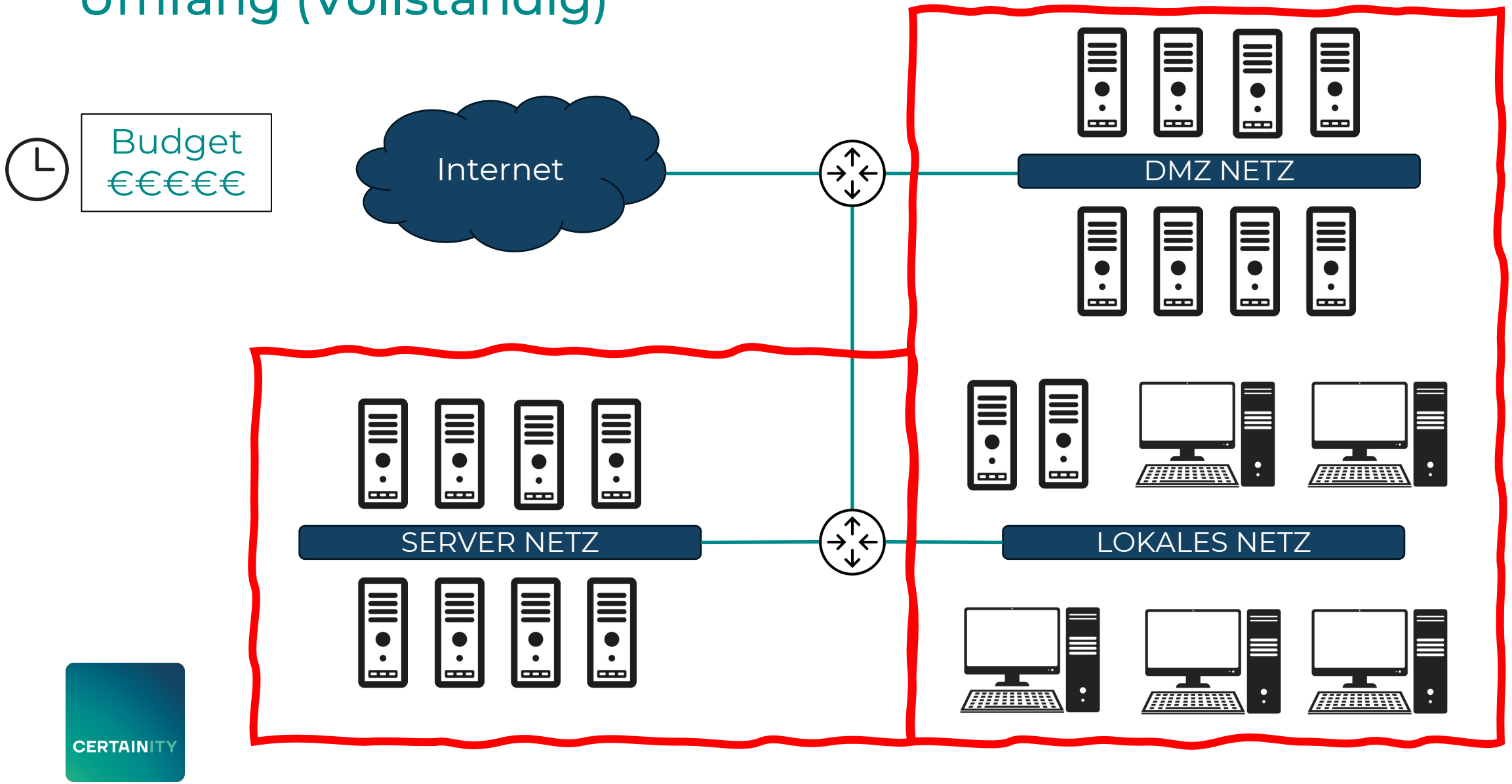


CERTAINITY

- Zielsetzung
- Scope
- Umfang
- Kenntnisstand
- Vorgehensweise & Tools

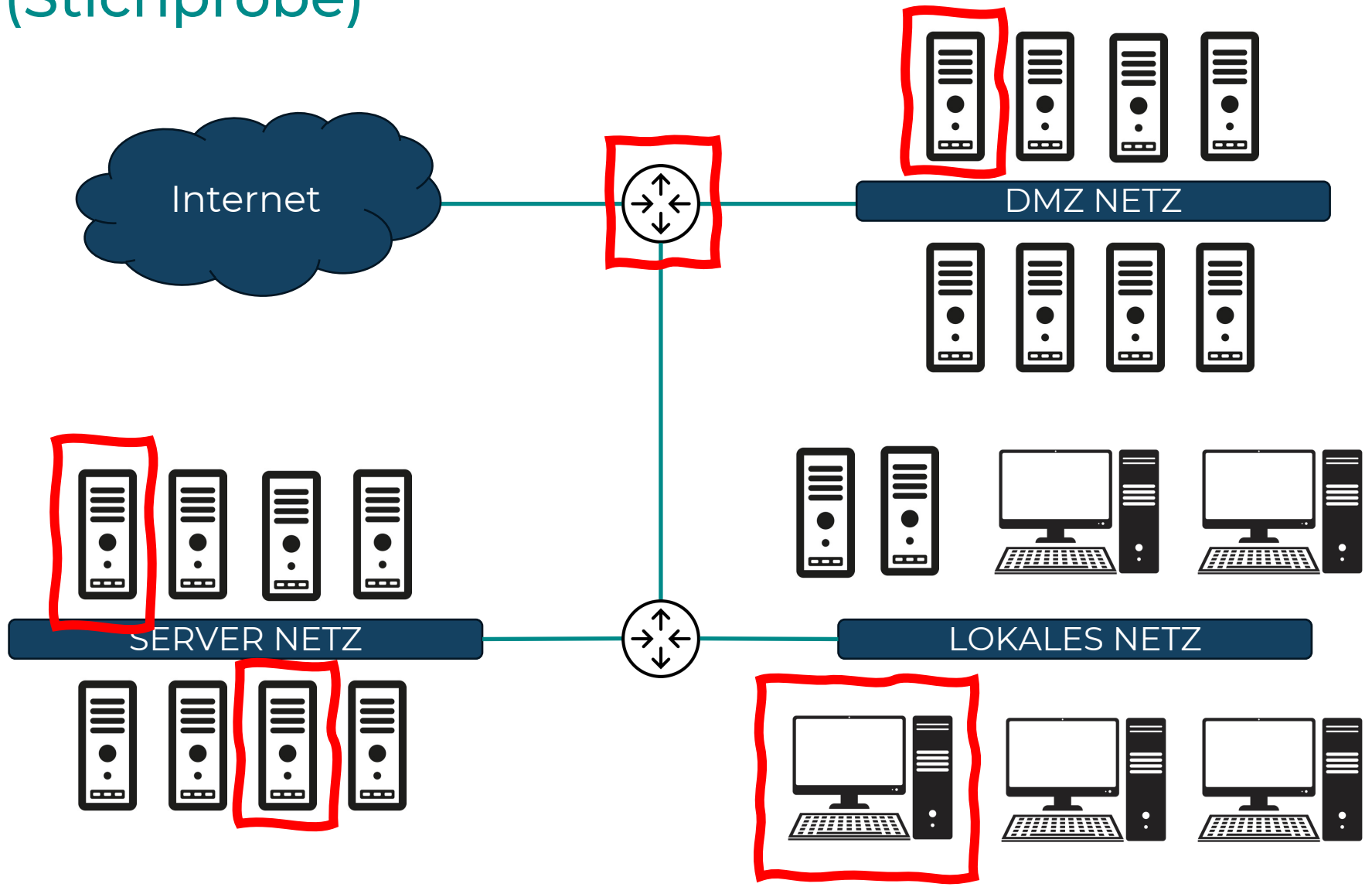
CERTAINITY

Umfang (Vollständig)



Umfang (Stichprobe)

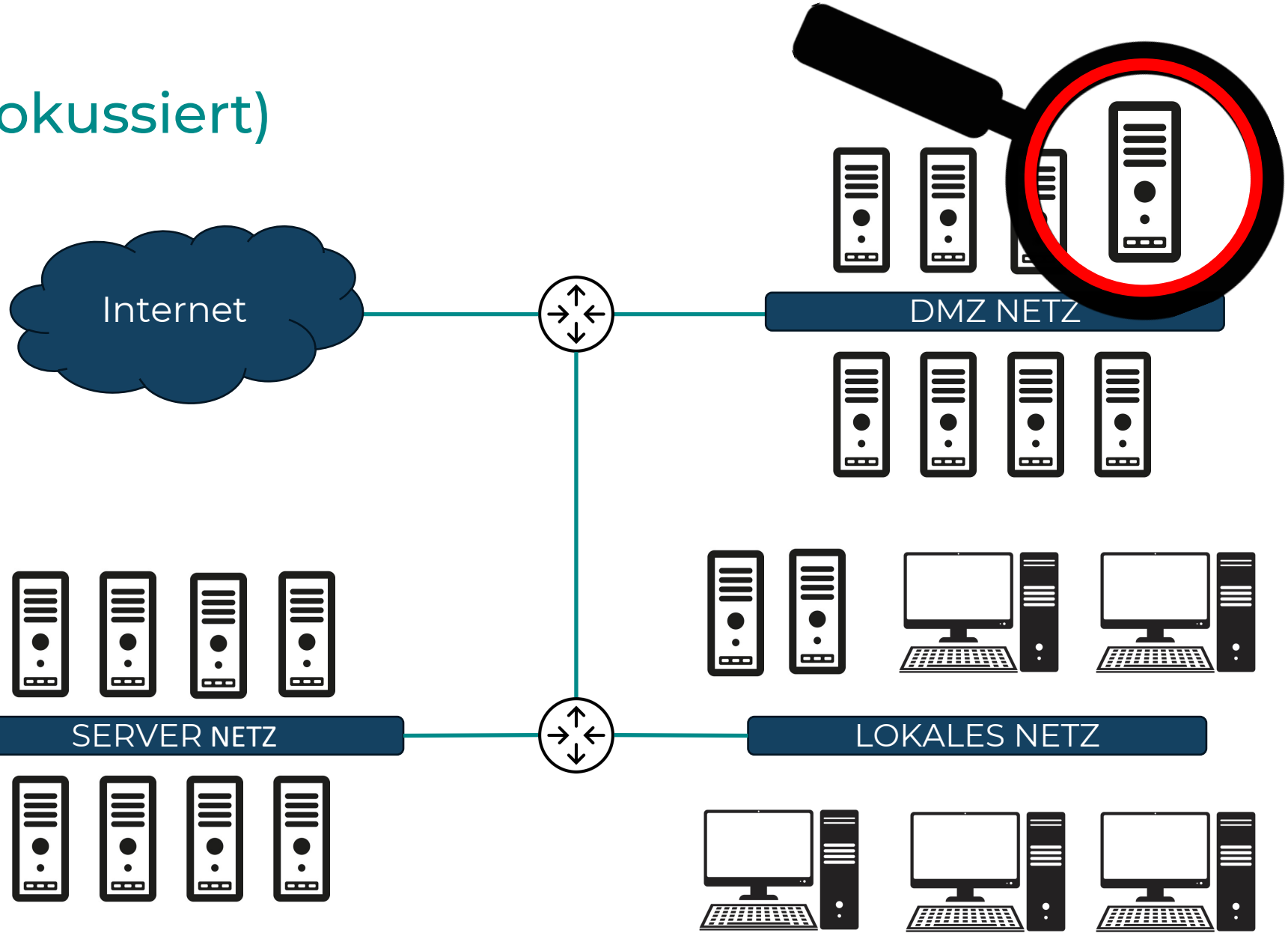
Budget
€ - €€€



CERTAINITY

Umfang (Fokussiert)

Budget
€€ - €€€



CERTAINITY

- Zielsetzung
- Scope
- Umfang
- Kenntnisstand
- Vorgehensweise & Tools

CERTAINITY

Kenntnisstand

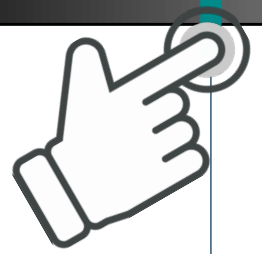
Blackbox

- Schnelle Durchführung
- Realistische Einschätzung
- Kostengünstiger
- Geringer Aufwände

Whitebox

- Sehr hoher Abdeckungsgrad beim Testen
- Maximale Detailierung bei der Identifikation von Schwachstellen
- Erhöhter Kommunikationsaufwand

Keine Kenntnisse — Informationstand über das Testobjekt — Volle Kenntnis



Greybox (Hybrid)

- Hoher Abdeckungsgrad beim Testen
- Gute Detailierung bei der Identifikation von Schwachstellen
- Leicht erhöhter Kommunikationsaufwand

CERTAINITY

- Zielsetzung
- Scope
- Umfang
- Kenntnisstand
- Vorgehensweise & Tools

CERTAINITY



Verdeckte Vorgehensweise

- Kreis der Informierten ist minimal
- Testmuster und Aktivitäten werden verschleiert
- Admin-, SoC oder Security Team sind nicht informiert
- Ziel ist es nicht entdeckt zu werden

Reaktionsfähigkeit des Security Teams prüfen

Testgeschwindigkeit ist reduziert

Erhöhter Aufwand durch Verschleierung

Offene Vorgehensweise

- Admin-, SoC oder Security Team sind informiert
- Mitarbeiter sind informiert

Stabiler Betrieb während des Tests (Team auf Standby)

Ziel ist es möglichst effizient zu testen

Tests der Reaktionsfähigkeit des Security Teams bei einem echten Angriff ist nicht möglich

Manuell

- Hohe Interaktivität
- Flexible und kreative Testmuster
- Schwankende Qualität je nach Auditor/Tag
- Höchste Testqualität –> Falses Positive Validierung, individuelle Risikoeinschätzung
- Mangelnde Verfügbarkeit und niedrige Skalierbarkeit
- Personalkosten

Automatisiert

- (fast) keine Interaktivität
- Standard-Testkatalog
- Exakt-Gleichbleibende Messung (keine Qualitätsschwankungen)
- Herausforderung bei False Positives und Risikoeinschätzung
- Niedrige Kosten und hohe Skalierbarkeit
- Lizenzkosten

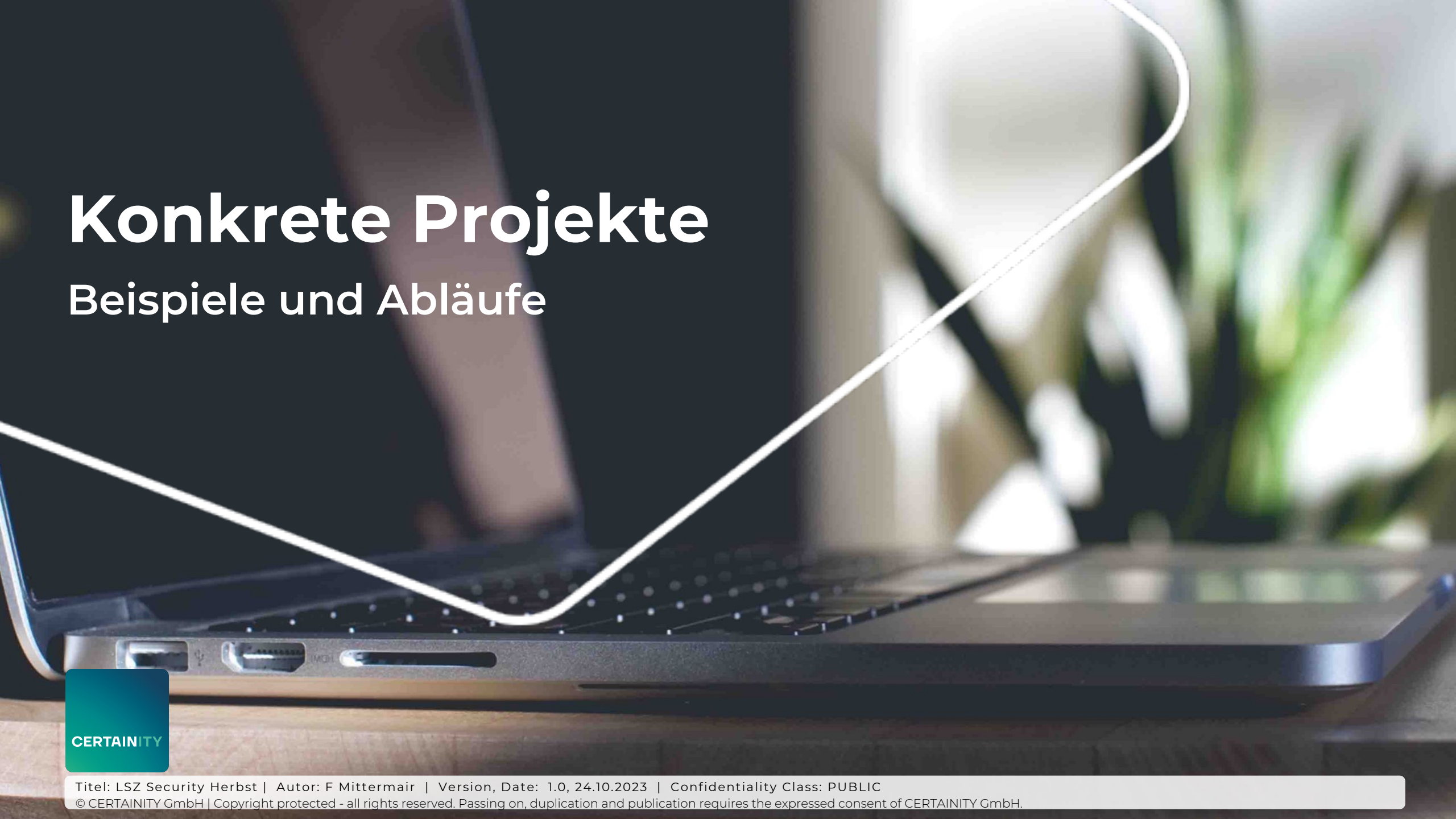
Autonom (AI)

- Gute Interaktivität
- Standardisierter Testkatlog und Ansätze von Kreativität
- Vergleichbare Messergebnisse
- Verbesserte False Positive Validierung und Risikoeinschätzung
- Gute Skalierbarkeit
- Lizenzkosten

Einschränkung: Reifegrad der Technologie

Konkrete Projekte

Beispiele und Abläufe



CERTAINITY

Penetration Test (Externe Systeme)

Fragestellung?

- Auf welchem IT-Sicherheits-Level ist meine IT Infrastruktur?
- Wie effektiv sind die implementierten Sicherheitsmaßnahmen die meine IT Systeme schützen?
- Können Cyber-Kriminelle meine Systeme infiltrieren und Schaden verursachen?

Zielsetzung

Bei einem Penetration Test (Extern) wird der Sicherheitsstatus aller über das Internet erreichbaren IT Systeme eines Unternehmens geprüft. Ziel ist es möglichst viele potenzielle Sicherheitslücken aufzudecken

Vorgehensweise

Information Gathering → Enumeration & Scanning → Evaluierung → Exploitation → Risk Analyse → Dokumentation

Nutzen

- Lösungsempfehlungen zu identifizierten Sicherheitslücken und in Folge dessen Steigerung des IT Sicherheitslevels
- Vertrauensbildung gegenüber Ihren Kunden, Partnern, Lieferanten und Mitarbeitern
- Einhaltung von Vorschriften, Standards und Compliance Anforderungen

Warum CERTAINITY?

✓ Individuelle Lösungen, pragmatische Methoden und Empfehlungen passend zu Ihrer Anforderung

Ergebnisse


Technische Zusammenfassung

In diesem Kapitel werden alle ermittelten Schwachstellen im Detail beschrieben, einschließlich ihrer spezifischen Risikobewertung, der Wahrscheinlichkeit ihres Auftretens und der empfohlenen Abhilfemaßnahmen. Zunächst wird eine Zusammenfassung aller entdeckten Schwachstellen angezeigt, danach wird jede einzelne Schwachstelle in separaten Kapiteln aufgeführt.

Zur besseren Orientierung des Lesers sind die Schwachstellen nach absteigender Kritikalität sortiert und mit einer passenden Testfallkategorie versehen.

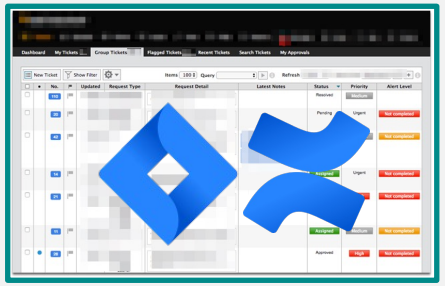
4.1 Zusammenfassung der Schwachstellen

Die folgende Tabelle gibt einen Überblick über die Themen, die im Rahmen dieser Bewertung behandelt wurden:

Vulnerability	Severity	Likelihood
Persistentes Cross-Site Scripting	Medium	Probable
Fehlende Patches und Einsatz von Software mit EOL	Critical	Probable
Netlogon Skripte mit VNC Passwort Netlogon Skripte mit VNC Passwort	Critical	Very Likely
Kritische Schwachstellen in der	Critical	Very Likely
	Critical	Very Likely
Lokale Administratoren mit wiederverwendetem Passwörter	Critical	Probable
Lokale Administratoren & Domain Admin mit gleichem Passwort	Critical	Probable
Einsatz von Domain Administratoren auf nicht Domain Controllern	Critical	Feasible
	Critical	Probable
Backup User mit Domain Admin Rechten	Critical	Very Likely
Netzwerksegmentierung	High	Probable

Streng vertraulich, Release Version Seite 10

Auditergebnisse in Form eines Abschlussberichts (PDF) inkl. Proof-of-Concept, Lösungsempfehlung und Risiko-Einschätzung



Optional:
Bereitstellung der Ergebnisse in Ihr eigenes Ticket-System (z.B. Jira) für eine optimale interaktive Zusammenarbeit bei der Behebung der Sicherheitsprobleme

Security Assessment spezifischer Anwendung

Fragestellung?

- Entspricht meine Anwendung in Bezug auf IT Sicherheit dem aktuellen Stand der Technik
- Können Cyber-Kriminelle Daten meiner Anwendung manipulieren und Schaden verursachen?
- Kann es zu einem Datenleck kommen?

Zielsetzung

Bei dem Security Assessment wird der Sicherheitsstatus einer ausgewählten Anwendung geprüft. Ziel ist es möglichst viele potenzielle Sicherheitslücken aufzudecken

Vorgehensweise

Information Gathering → Enumeration & Scanning → Evaluierung → Exploitation → Risk Analyse → Dokumentation

Nutzen

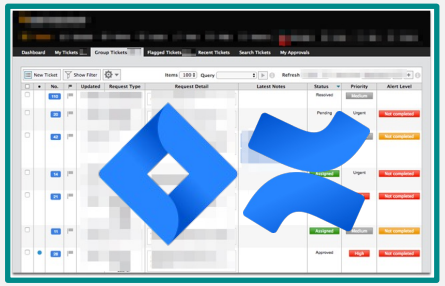
- Lösungsempfehlungen zu identifizierten Sicherheitslücken und in Folge dessen Steigerung des IT Sicherheitslevels
- Vertrauensbildung gegenüber Ihren Kunden, Partnern, Lieferanten und Mitarbeitern
- Einhaltung von Vorschriften, Standards und Compliance Anforderungen

Warum CERTAINITY?

✓ Individuelle Lösungen, pragmatische Methoden und Empfehlungen passend zu Ihrer Anforderung

Ergebnisse

Auditergebnisse in Form eines Abschlussberichts (PDF) inkl. Proof-of-Concept, Lösungsempfehlung und Risiko-Einschätzung



Optional:
Bereitstellung der Ergebnisse in Ihr eigenes Ticket-System (z.B. Jira) für eine optimale interaktive Zusammenarbeit bei der Behebung der Sicherheitsprobleme

Red Team Engagement

Fragestellung?

Ist meine Organisation einem vollständigen Cyber Angriff gewachsen?

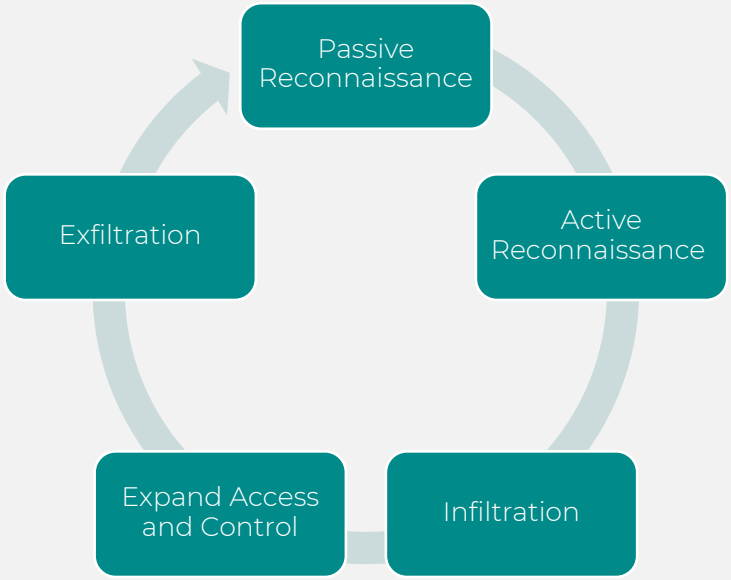
Zielsetzung

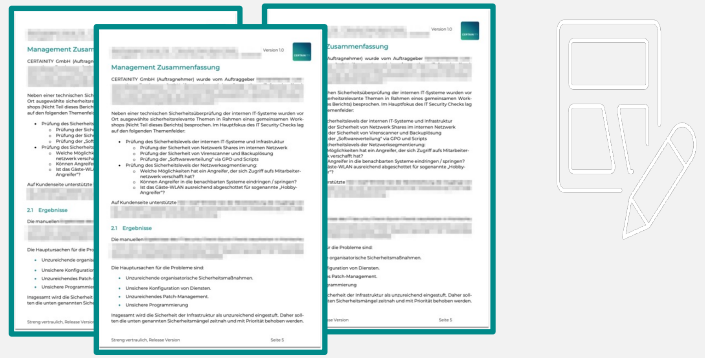
Durchführung eines realistischen Cyber Angriffs um das allgemeine Sicherheitslevel und die Reaktionsfähigkeit sowie Effektivität der Cyber Verteidigung (Blue Team) eines Unternehmens zu testen

Vorgehensweise

Bei einem Red Team Engagement handelt sich um die Simulation eines APT (advanced Persitent threat) Cyberangriffs bei dem man sich der Techniken, Taktiken und Vorgehensweisen (TTPs) von Cyber Kriminellen bedient.

Für die Modellierung der identifizierten Bedrohungen verwenden wir das Rahmenwerk von MITRE ATT&CK. Dies erleichtert die Kommunikation und Zusammenarbeit mit dem Blue Team bzw. dem IT Management





Im Zuge des Projekts werden Angriffsszenarien vorbereitet und durchgeführt. Das Vorgehen und der jeweilige Ausgang wird in einem Abschluss Report dokumentiert

Ergebnisse

CERTAINITY

Warum CERTAINITY?

- ✓ Individuelle Lösungen, pragmatische Methoden und Empfehlungen

Nutzen

- Strategische Empfehlungen um die IT Security der Organisation zu heben
- Kenntnis über Reaktionsfähigkeit und Effektivität des eigenen Blue Team
- Training für die Blue Teams auf Basis eines individuell gewählten Szenarios

Titel: LSZ Security Herbst | Autor: F Mittermair | Version, Date: 1.0, 24.10.2023 | Confidentiality Class: PUBLIC

Sie sind auf der Suche nach einem Partner für Penetration Tests, Sicherheitsüberprüfungen und Cyber Security Beratung?

Ihr direkter Draht zu uns

Mag. (FH) **Theresa Mosing**

Head of Sales

Mail: theresa.mosing@certainity.com

Ulrich Fleck

CEO

Mail: ulrich.fleck@certainity.com

Fabian Mittermair

Head of Offensive Security

Mail: fabian.mittermair@certainity.com

CERTAINITY

CERTAINITY

CERTAINITY GmbH

reliable. trustworthy. bespoke.

HEILIGENSTÄDTER LÄNDE 27c | A – 1190 WIEN
HG WIEN, FN 262176 D | FIRMENSITZ: WIEN

office@certainity.com
https://certainity.com